National Infrastructure Protection Center CyberNotes

Issue #2002-16 *August 12, 2002*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, malicious scripts, information security trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between July 18 and August 8, 2002. The table provides the vendor, operating system, software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates to items appearing in previous issues of CyberNotes are listed in bold. New information contained in the update will appear in italicized colored text.** Where applicable, the table lists a "CVE number" (in red) which corresponds to the Common Vulnerabilities and Exposures (CVE) list, a compilation of standardized names for vulnerabilities and other information security exposures.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Adobe[1]	Windows, MacOS 9	eBook Reader for Mac OS 9 2.1, 2.2, Windows 2.1, 2.2	A vulnerability exists in the encryption scheme used for the challenge/response cycle, which could let a malicious user transfer an eBook to a different computer.	No workaround or patch available at time of publishing.	eBook Reader File Transfer Authorization	Medium	Bug discussed in newsgroups and websites.

[1] Securiteam, July 31, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Aprelium Technologies[2]	Windows NT	Abyss Web Server 1.0.3	A vulnerability exists when a malformed GET command is received, which could let a malicious user obtain sensitive information.	Upgrade available at: http://www.aprelium.com/data/abws107.exe	Abyss Web Server HTTP GET Request	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
ArGoSoft[3]	Windows NT 4.0/2000, XP	Mail Server Pro 1.8.1.6, 1.8.1.5, 1.8.1.7	A Denial of Service vulnerability exists when a remote malicious user creates a mail-loop condition.	No workaround or patch available at time of publishing.	Mail Server Pro Remote Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Avaya[4]	Multiple	Cajun M770 Supervisor Firmware 3.3, M770-ATM Series Firmware 2.3.11, P130 Series Firmware 2.9.1, P330 Series Firmware 3.8.1, 3.8.2, 3.9.1, 3.10	A vulnerability exists in the community string, which could let a remote malicious to view/set potentially sensitive properties within the device and obtain unauthorized administrative access.	Upgrade available at: http://support.avaya.com/japple/css/japple?temp.groupID=125615&temp.selectedFamily=125618&temp.selectedProduct=107702&temp.selectedBucket=all&temp.feedbackState=askForFeedback&temp.documentID=126909&PAGE=avaya.css.CSSLvl1Detail&aClass=japple.web.services.DataTransactionService(runStatement,avaya.css.UsageUpdate)	Cajun Firmware Default Community String	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Ben Chivers[5]	Unix	Easy Guestbook 1.0	Several vulnerabilities exist: a vulnerability exists due to inadequate authentication, which could let a malicious user delete entries and login as an administrator; and a vulnerability exists in 'config.cgi,' which could let a malicious user change the Admin password and reconfigure Guestbook.	No workaround or patch available at time of publishing.	Easy Guestbook Administrative Access	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Ben Chivers[6]	Unix	Easy Homepage Creator 1.0, Advanced Easy Homepage Creator 1.0	A vulnerability exists due to inadequate authentication, which could let a malicious user modify a user's homepage.	No workaround or patch available at time of publishing.	Easy Homepage Creator Inadequate Authentication	Medium	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[2] Bugtraq, July 29, 2002.
[3] Bugtraq, August 4, 2002.
[4] Avaya Security Advisory, July 22, 2002.
[5] AresU Advisory, July 19, 2002.
[6] AresU Advisory, July 18, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Bharat Mediratta[7]	Unix	Gallery 1.1-1.3	A vulnerability exists in several of the PHP script files due to improper variable checking, which could let a remote malicious user execute arbitrary code.	Upgrade available at: http://jpmullan.com/galleryupdates/daily/current.gallery.tar.gz **Debian:** http://security.debian.org/pool/updates/main/g/gallery/	Gallery Remote File Include	**High**	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.
Brother[8]	Multiple	NC-3100h	A Denial of Service vulnerability exists when a malicious user submits an oversized administrative password via the web interface.	No workaround or patch available at time of publishing.	NC-3100H Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Cerulean Studios[9]	Windows 95/98/ME/NT 4.0/2000	Trillian 0.73, 0.725, 0.6351	Two vulnerabilities exist: a format string vulnerability exists due to the way channel invites are handled, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability exists in the DCC chat module due to insufficient bounds checking, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Trillian Buffer Overflows	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Cisco Systems[10]	Multiple	IntraPort 2, 2+, Carrier-2, Carrier-8, Enterprise-2, 8, VPN 5001 Concentrator, VPN 5002 Concentrator, VPN 5008 Concentrator	A vulnerability exists because the client password is sent in plaintext when Password Authentication Protocol (PAP) or Challenge (a hybrid of PAP) is used and more than one authentication message is transmitted, which could let a malicious user obtain sensitive information. *Note: This issue does not exist if CHAP authentication is used.*	Information on obtaining updated software is available at: http://www.cisco.com/univercd/cc/td/doc/product/aggr/vpn5000/5000sw/conce60x/5000cfg/swinst.htm	VPN 5000 Concentrator Plaintext	Medium	Bug discussed in newsgroups and websites. Vulnerability may be exploited with available tools.
Cisco Systems[11]	Multiple	IOS 11.1-11.3	A buffer overflow vulnerability exists in the Trivial File Transfer Protocol (TFTP) server file name due to insufficient bounds checking on requested file names, which could let a remote malicious user cause a Denial of Service.	Workaround available at: http://www.cisco.com/warp/public/707/ios-tftp-long-filename-pub.shtml	IOS TFTP Buffer Overflow	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[7] Debian Security Advisory, DSA-138-1, August 1, 2002.
[8] Phenoelit Advisory, July 27, 2002.
[9] Securiteam, August 5, 2002.
[10] Cisco Security Advisory, August 7, 2002.
[11] Cisco Security Advisory, July 30, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Compaq Computer Corporation[12] ***Patches now available***[13]	**Unix**	**Tru64 5.0, 5.0 a, 5.1, 5.1 a**	**A buffer overflow vulnerability exists in the 'su' utility due to insufficient bounds checking, which could let a malicious user execute arbitrary instructions as root.**	***Patches available at:*** ***http://ftp.support.compaq.com/patches/public/unix/***	**Tru64 SU Buffer Overflow**	**High**	**Bug discussed in newsgroups and websites. Exploit scripts have been published.** ***Vulnerability has appeared in the press and other public media.***
Compaq Computer Corporation[14]	Unix	Tru64 4.0g, 4.0f, 5.0a, 5.1a, 5.1	Several vulnerabilities exist: a vulnerability exists in the 'chsh' utility, which could let a malicious user obtain root privileges; a vulnerability exists in 'passwd,' which could let a malicious user obtain root privileges; a vulnerability exists in 'chfn,' which could let a malicious user obtain root privileges; and a vulnerability exists in 'dxchpwd,' which could let a malicious user obtain root privileges.	Patches available at: http://ftp.support.compaq.com/patches/public/unix/	Tru64 Multiple Vulnerabilities	**High**	Bug discussed in newsgroups and websites.
D-Link[15]	Multiple	DP-303	A Denial of Service vulnerability exists when a malicious user sends an excessively long post request to a configuration page.	No workaround or patch available at time of publishing.	D-Link Denial of Service	Low	Bug discussed in newsgroups and websites.
Dotmarketing.org[16]	Unix	DotProject 0.2.1 .5	A vulnerability exists because the software relies on the user 'cookie_value' for authentication, which could let a remote malicious user bypass authentication and obtain administrative access.	No workaround or patch available at time of publishing.	DotProject Authentication Bypass	**High**	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Endity.com[17]	Multiple	ShoutBox 1.2	A vulnerability exists because HTML tags are not sufficiently sanitized from input supplied via form fields, which could let a malicious user execute arbitrary HTML and script.	No workaround or patch available at time of publishing.	ShoutBox HTML Injection	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[12] Bugtraq, July 19, 2002.
[13] Compaq Security Bulletin, SSRT2257, August 5, 2002.
[14] Compaq Security Bulletin, SSRT2257, August 5, 2002.
[15] Phenoelit Advisory, July 27, 2002
[16] SCAN Associates Sdn Bhd Security Advisory, July 29, 2002.
[17] Bugtraq, July 29, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Ensim[18]	Multiple	Web-ppliance 3.0, 3.1	A vulnerability exists because users' e-mail aliases are incorrectly processed, which could let a malicious user receive other users' e-mails.	No workaround or patch available at time of publishing.	Webppliance Unauthorized E-mail Access	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Fake Identd[19]	Unix	Fake Identd 0.9 b, 0.9, 1.1-1.4	A buffer overflow vulnerability exists due to a failure to properly handle long client requests, which could let a remote malicious user execute arbitrary code with root privileges.	Upgrade available at: http://www.guru-group.fi/~too/sw/releases/identd.c	Fake Identd Client Query Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Frederic Tyndiuk[20]	Unix	Eupload 1.0	A vulnerability exists because passwords are stored in plain text, which could let a remote malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Eupload Plain Text Password Storage	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
FreeBSD [21]	Unix	FreeBSD 4.0-4.6, 4.1.1 – 4.6 STABLE 4.1.1 – 4.3 RELEASE, 4.5-4.6 RELEASE, 4.3 – 4.4 RELENG	A vulnerability exists in the maximum permitted Fast File System (FFS) file size calculation, which could let a malicious user read and write arbitrary files on local filesystems, allowing them to obtain superuser privileges.	Patch available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-02:35/ffs.patch	FreeBSD Arbitrary FFS Filesystem	**High**	Bug discussed in newsgroups and websites.
FreeBSD [22]	Unix	FreeBSD 4.0-4.6, 4.1.1 – 4.6 STABLE 4.1.1 – 4.3 RELEASE, 4.5-4.6 RELEASE, 4.3 – 4.4 RELENG	A Denial of Service vulnerability exists in the implementation of NFS due to improper handling of certain incoming RPC messages.	Patch available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-02:36/nfs.patch	FreeBSD NFS Denial of Service	Low	Bug discussed in newsgroups and websites.

[18] SecurityFocus, August 7, 2002.
[19] Bugtraq, July 29, 2002.
[20] Securiteam, July 31, 2002.
[21] FreeBSD Security Advisory, FreeBSD-SA-02:35, August 5, 2002.
[22] FreeBSD Security Advisory, FreeBSD-SA-02:36, August 6, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
FreeBSD [23]	Unix	FreeBSD 4.3 – RELEASE, 4.4 – STABLE, 4.4 – RELENG, 4.4, 4.5 – STABLE, 4.5 – RELEASE, 4.5, 4.6 – STABLE, 4.6 – RELEASE, 4.6	A Denial of Service vulnerability exists in the kqueue mechanism when an event is associated with a pipe that has been half closed.	Patch available at: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-02:37/kqueue.patch	FreeBSD kqueue Denial of Service	Low	Bug discussed in newsgroups and websites.
Google[24]	Multiple	Toolbar 1.1.41-1.1.45, 1.1.47-1.1.49, 1.1.53-1.1.58	Multiple vulnerabilities exists a vulnerability exists because it is possible to modify configuration settings by visiting a specific URL that accepts commands as CGI parameters, which could let a malicious user modify the toolbar configuration and execute arbitrary script code within the Local System security zone; and a vulnerability exists because keypress events can be sent to a malicious browser window, which could let a malicious user monitor these events and access whatever is typed into the toolbar.	Update available at: http://toolbar.google.com/	Google Toolbar Multiple Vulnerabilities	Medium/ **High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Exploits have been published.
Hewlett Packard Systems[25]	Multiple	Business Inkjet 2600, color LaserJet 4550, Designjet 5000, LaserJet 4100, 8150, 9000	A vulnerability exists in the Embedded Web Server (EWS) because passwords are handled in an insecure manner, which could let a remote malicious user cause a Denial of Service or obtain unauthorized access.	Upgrade available at: http://itrc.hp.com	JetDirect Embedded Web Server	Low/ Medium (Medium if unauthorized access is obtained)	Bug discussed in newsgroups and websites.
Hewlett Packard Systems[26]	Multiple	ProCurve Switch 4000M	A Denial of Service vulnerability exists when a malicious user issues a special SNMP Write command.	No workaround or patch available at time of publishing.	ProCurve Switch Denial of Service	Low	Bug discussed in newsgroups and websites. Proof of Concept exploit has been published.

[23] FreeBSD Security Advisory, FreeBSD-SA-02:37, August 6, 2002.
[24] GreyMagic Security Advisory, GM#001-MC, August 8, 2002.
[25] Hewlett-Packard Company Security Advisory, HPSBUX0207-204, July 31, 2002.
[26] Securiteam, July 28, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hewlett Packard Systems[27]	Multiple	ChaiVM	Two vulnerabilities exist: a vulnerability exists due to inadequate access control enforcement, which could let a malicious user modify, add, and delete services; and a vulnerability exists because EZLoader does not sufficiently validate JAR signatures of services prior to loading them, which could let a malicious user replace a legitimate service with a malicious version.	No workaround or patch available at time of publishing.	ChaiVM Arbitrary Service Modification & JAR Signature Validation	Medium	Bug discussed in newsgroups and websites.
Hewlett Packard Systems[28]	Unix	HP-UX 11.0 4, 11.0, 11.11	A Denial of Service vulnerability exists in the ptrace system call due to an incorrect reference to a thread register state.	Patches available at: http://itrc.hp.com PHKL_27536, PHKL_27180, PHKL_27179	HP-UX PTrace Denial of Service	Low	Bug discussed in newsgroups and websites.
Hewlett Packard Systems[29]	Multiple	JetDirect x.21.00, x.20.00, x.08.32, x.08.20, x.08.05, x.08.04, x.08.00, JetDirect J3111A rev. G.08.03, G.07.17, G.07.03, G.07.02, G.05.35, A.08.06	A vulnerability exists when an SNMP READ request is sent to the printer, which could let a remote malicious user obtain sensitive information, and access and change the configuration of the printer.	No workaround or patch available at time of publishing.	JetDirect Administrative Password Retrieval	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.

[27] Securiteam, July 28, 2002.
[28] Hewlett-Packard Company Security Bulletin, HPSBUX0208-206, August 6, 2002.
[29] Phenoelit Advisory, July 27, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Hewlett Packard Systems[30]	Windows NT 4.0/2000, Unix	OpenView Emanate SNMP Agent 14.2 Win NT/2k, Solaris 2.X, HP-UX 11.X, 10.20	A vulnerability exists because a default community string is used that is predictable, which could let a malicious user obtain unauthorized access or cause a Denial of Service.	Upgrades available at: NNM_00936.EXE http://support.openview.hp.com/cpe/cgi-bin/saveAs?productName=/emanate/14.2/intelNT_4.X/NNM_00936.EXE PSOV_03193 http://support.openview.hp.com/cpe/cgi-bin/saveAs?productName=/emanate/14.2/sparc_2.X/PSOV_03193 PHSS_27570 http://support.openview.hp.com/cpe/cgi-bin/saveAs?productName=/emanate/14.2/s700_800_11.X/PHSS_27570 PHSS_27569 http://support.openview.hp.com/cpe/cgi-bin/saveAs?productName=/emanate/14.2/s700_800_10.X/PHSS_27569	EMANATE 14.2 Predictable SNMP Community String	Low/ Medium (Medium if unauthor-ized access is obtained)	Bug discussed in newsgroups and websites. Vulnerability may be exploited using a SNMP client.
Hylafax[31]	Unix	Hylafax 4.0 pl2, 4.0 pl1, 4.0 pl0, 4.0.2, 4.1, 4.1 - beta1-3, 4.1.1, 4.1.2	Multiple vulnerabilities exist: a Denial of Service vulnerability exists in the Transmitting Subscriber Identification (TSI) string due to improper sanitization of user input; and a buffer overflow vulnerability exists when a malicious fax includes a long scan line, which could let a malicious user cause a Denial of Service or possibly execute arbitrary code with root privileges.	Upgrade available at: ftp://ftp.hylafax.org/source/hylafax-4.1.3.tar.gz	Hylafax Multiple Vulnerabilities	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites.
Imatix[32]	Windows NT	Xitami version 2.5b5	A Denial of Service vulnerability exists when a remote malicious user makes a large number of connections.	No workaround or patch available at time of publishing.	Xitami Connection Flood Denial of Service	Low	Bug discussed in newsgroups and websites.
Inso[33]	Unix	dwhttpd 4.0.2 a7a, 4.1 a6	A format string vulnerability exists when requests for nonexistent files are logged, which could let a remote malicious user execute arbitrary code.	Patches available at: http://sunsolve.sun.com:	DynaWeb httpd Format String	**High**	Bug discussed in newsgroups and websites.

[30] Hewlett-Packard Company Security Bulletin, HPSBUX0208-208, August 8, 2002.
[31] HylaFAX.org Security Advisory, July 29, 2002.
[32] Securiteam, August 5, 2002.
[33] Bugtraq, August 1, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Inter7[34]	Multiple	qmailadmin 1.0.1, 1.0.2	A buffer overflow vulnerability exists when an environment variable is processed due to improper bounds checking, which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	qmailadmin Buffer Overflow	Medium	Bug discussed in newsgroups and websites. Exploit script has been published.
IpSwitch[35]	Windows NT 4.0/2000, XP	WS FTP Server 3.1.1	A buffer overflow vulnerability exists in the CPWD command that is used to modify an authenticated user's password, which could let a remote malicious user execute arbitrary code.	Upgrade available at: ftp://ftp.ipswitch.com/ipswitch/product_support/WS_FTP_Server/ifs312.exe	IpSwitch CPWD Remote Buffer Overflow CVE Name: CAN-2002-0826	**High**	Bug discussed in newsgroups and websites.
IpSwitch[36]	Windows NT 3.5.1/4.0/ 2000, XP	IMail 6.0, 6.0.1-6.0.6, 6.1-6.4, 7.0.1-7.0.7	A Denial of Service vulnerability exists when a HTTP POST command is made to the web calendaring service on port 8484, and the "content-length:" header field is blank.	No workaround or patch available at time of publishing.	IMail Web Calendaring Denial of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Jacob Navia[37]	Windows 95/98/ME	lcc-Win32 3.2	A vulnerability exists because memory is not initialized before it is written to a disk, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	LCC-Win32 Compiled Binary Memory Disclosure	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
John G. Myers[38]	Unix	Mpack 1.5	Several vulnerabilities exist: a buffer overflow vulnerability exists in the MUnpack program when a malformed e-mail or NNTP article is sent, which could let a malicious user cause a Denial of Service and possibly execute arbitrary code; and a vulnerability exists if a MIME encoded message is sent that contains an attachment that refers to a malformed filename, which could let a malicious user decode the attachment outside of a designated directory.	**Debian:** http://security.debian.org/pool/updates/main/m/mpack/mpack/	Mpack Buffer Overflow & Malformed Filename	Low/ **High** **(High if arbitrary code is executed)**	Bug discussed in newsgroups and websites.
LibPNG [39]	Unix	LibPNG 1.0.12	A vulnerability exists due to the way overly wide images are handled, which could let a malicious user execute arbitrary code.	**Debian:** http://security.debian.org/pool/updates/main/libp/libpng3	LibPNG Wide Image Processing	**High**	Bug discussed in newsgroups and websites.

[34] SecurityFocus, August 6, 2002.
[35] @stake, Inc. Security Advisory, a090902-1, August 8, 2002.
[36] Bugtraq, July 30, 2002.
[37] Securiteam, August 5, 2002.
[38] Debian Security Advisory DSA 141-1, August 1, 2002.
[39] Debian Security Advisory, DSA 140-2, August 5, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Lucent Technologies[40]	Multiple	Access Point 1500 Service Router, 300 Service Router , 600 Service Router	A Denial of Service vulnerability exists when a malicious user sends a HTTP request containing 4000 characters.	No workaround or patch available at time of publishing.	Lucent Access Point IP Services Router Long HTTP Request Denial Of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.
Lucent Technologies[41]	Multiple	Ascend MAX 5.0 .0Ap42, Pipeline 5.0.0A, MAX Router 1.0-5.0, 5.0 ap48, Pipeline Router 1.0-6.0, 6.0.2, DSL Terminator	A vulnerability exists when a specially crafted packet is sent to some configuration devices on UDP port 9, which could let a malicious user obtain sensitive information and a remote malicious user change the devices' IP address, netmask, or name.	No workaround or patch available at time of publishing.	Multiple Lucent Router UDP Port 9 Information Disclosure	Medium	Bug discussed in newsgroups and websites.
Lucent Technologies[42]	Multiple	VPN Firewall Brick 1000, 20, 201, 80	Multiple vulnerabilities exist: a Denial of Service vulnerability exists if a malicious user interrupts a connection between the Brick and critical devices such as the LSMS (Brick Management Server); a Denial of Service vulnerability exists because ARP traffic is forwarded across interfaces regardless of any defined firewall ruleset; and a vulnerability exists because the all Bricks are identifiable during reconnaissance, which could let a malicious user obtain sensitive information.	**Lucent's Response:** "The Lucent VPN Firewall Brick version 6.0 can be configured to be not vulnerable to the types of attacks specified in this advisory notification." VPN Firewall 7.0 will provide additional security features that mitigate this issue and is scheduled for release in September 2002.	Lucent Brick Multiple Vulnerabilities	Low/ Medium (Medium if sensitive information can be obtained)	Bug discussed in newsgroups and websites. There is no exploit code required.
Macromedia[43]	Windows 95/98/ME/NT 4.0/2000, XP, Unix	Flash 5.0, 6.0, 6.0.29.0	A buffer overflow vulnerability exists in Flash Shockwave movie files (.SWF) due to insufficient bounds checking of headers, which could let a remote malicious user execute arbitrary code.	Upgrades available at: http://www.macromedia.com/shockwave/download/frameset.fhtml?P1_Prod_Version=ShockwaveFlash Flash 5.0r50 (Linux) http://www.macromedia.com/go/getflashplayer/	Flash Malformed Header Buffer Overflow	**High**	Bug discussed in newsgroups and websites.

[40] Securiteam, July 30, 2002.
[41] Securiteam, July 28, 2002.
[42] Phenoelit Advisory, July 27, 2002.
[43] eEye Digital Security Advisory, August 8, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Macromedia[44]	Multiple	Flash 6.0, 6.0.29.0, 6.0.40.0	A vulnerability exists due to the way flash animations are handled, which could let a malicious user obtain sensitive information.	Upgrade available at: http://www.macromedia.com/shockwave/download/frameset.fhtml?P1_Prod_Version=ShockwaveFlash	Flash Player Arbitrary Local File Access	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Microsoft[45]	Windows 2000	Exchange Server 2000, Exchange Server 2000 SP1&2	A Denial of Service vulnerability exists because IIS incorrectly allocates licenses to Exchange.	No workaround or patch available at time of publishing.	Exchange 2000 License Allocation Denial of Service	Low	Bug discussed in newsgroups and websites. Vulnerability may be exploited with a publicly available tool.
Microsoft[46]	Windows 2000	Exchange Server 2000, Exchange Server 2000 SP1&2	A Denial of Service vulnerability exists when a malicious user sends a malformed Microsoft Remote Procedure Call (MSRPC).	No workaround or patch available at time of publishing.	Exchange 2000 Multiple MSRPC Denial of Service	Low	Bug discussed in newsgroups and websites. Vulnerability may be exploited with a publicly available tool.
Microsoft[47]	Windows NT 4.0/2000	SQL Server 2000, SQL Server 2000 SP1&2	A buffer overflow vulnerability exists due to a default system configuration, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	SQL Server Remote Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Microsoft[48]	Windows NT 4.0/2000, XP	Content Management Server 2001, Content Management Server 2001 SP1	Several vulnerabilities exist: a buffer overflow vulnerability exists in a user authentication function, which could let a remote malicious user execute arbitrary code; a vulnerability exists as a result of two flaws in the MCMS Authoring function regarding how requests are authenticated and due to the way the web authoring function uploads files, which could let a remote malicious cause arbitrary files to be executed; and a SQL injection vulnerability exists in the MCMS Resource Request function, which could let a malicious user execute arbitrary system commands.	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-041.asp	Multiple Microsoft Content Management Server 2001 Vulnerabilities CVE Names: CAN-2002-0700, CAN-2002-0718, CAN-2002-0719	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

[44] Macromedia Advisory, MPSB02-10, August 8, 2002.
[45] Bugtraq, August 6, 2002.
[46] Bugtraq, August 6, 2002.
[47] Bugtraq, August 6, 2002.
[48] Microsoft Security Bulletin, MS02-041, August 7, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[49]	Windows NT 4.0/2000, XP	Windows 2000 Advanced Server, SP1&2, Datacenter Server, SP1&2, Professional, SP1&2, 2000 Server, SP1&2, 2000 Server Japanese Edition, 2000 Terminal Services, SP1&2, NT Enterprise Server 4.0, SP1-SP6a, NT Server 4.0, SP1-SP6a, NT Terminal Server 4.0, SP1-SP6a, NT Workstation 4.0, SP1-SP6a, Windows XP, 64-bit Edition, Home, Professional	A design error exists in the Win32 API inter-window message passing system, which could let a malicious user obtain elevated privileges.	No workaround or patch available at time of publishing.	Microsoft Windows Message Subsystem Design Error	Medium	Bug discussed in newsgroups and websites. Exploit script has been published. Vulnerability has appeared in the press and other public media.
Microsoft[50]	Windows NT	Windows 2000 Terminal Services SP1&2, 2000 Terminal Services	A Denial of Service vulnerability exists when a remote malicious user scans the server using NMap utilizing its SYN scan method.	No workaround or patch available at time of publishing.	Microsoft Windows Terminal Services Denial Of Service	Low	Bug discussed in newsgroups and websites. There is no exploit code required.

[49] Bugtraq, August 6, 2002.
[50] Securiteam, August 1, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[51]	Windows 2000	Windows 2000 Advanced Server, SP1&2, 2000 Datacenter Server, SP1&2, 2000 Professional, SP1&2, 2000 Server, SP1&2, 2000 Terminal Services, SP1&2	A vulnerability exists because read and write access is provided to the system partition under default installs, which could let a malicious user delete sensitive system files and create Trojaned files with the same name.	No workaround or patch available at time of publishing.	Microsoft Windows 2000 Insecure Default File Permissions	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Microsoft[52]	Windows 98/NT 4.0/2000, XP	MDAC 1.5, 2.0, 2.1 Upgrade, 2.1 Clean, 2.1 2.4202.3 (GA) clean, 2.1 2.4202.3 (GA), 2.1.1.3711.11 (GA), 2.5, 2.5 SP1&2, 2.5 RTM, 2.6, 2.6 SP1&2, 2.6 RTM, 2.7, 2.7 RTM Refresh	A buffer overflow vulnerability exists in the T-SQL OpenRowSet command, which could let a malicious user obtain complete control over the database, and potentially obtain administrative privileges. *Note: This issue is only exploitable if SQL Server is installed on a vulnerable system.*	Frequently asked questions regarding this vulnerability and the patch can be found at: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-040.asp	Microsoft Data Access Components T-SQL Buffer Overflow CVE Name: CVE-CAN-2002-0695	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Microsoft[53]	Windows 95/98/ME/NT 4.0/2000, XP, MacOS 7.0/7.0.1/7.1/7.1.2/7.5.1/7.5.2/7.5.3/7.6/7.6.1/8.0, Unix	Windows Media Player XP, 6.3, 6.4, 7.0, 7.1	A buffer overflow vulnerability exists when the exe is called with a file name equal to or longer than 279 characters, which could let a malicious user overwrite EIP.	Microsoft will address this issue in Windows XP Service Pack 1.	Windows Media Player Filename Buffer Overflow	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[51] Bugtraq, August 5, 2002.
[52] Microsoft Security Bulletin, MS02-040, July 31, 2002.
[53] Bugtraq, July 30, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft [54]	Windows 95/98/ME/NT 4.0/2000	Internet Explorer 5.0, 5.0.1, 5.0.1 SP1&2, 5.5, 5.5 SP1&2, 6.0	A vulnerability exists due to the way SSL certificates are handled, which could let a malicious user create SSL certificates for arbitrary domains that will be treated as trusted by the vulnerable browser.	No workaround or patch available at time of publishing.	Internet Explorer Invalid SSL Certificate Chain	Medium	Bug discussed in newsgroups and websites.
Microsoft [55]	Windows	Outlook Express 6.0	A vulnerability exists due to the way script code that is included in XSL style information is treated, which could let malicious XML file attachments execute arbitrary code.	No workaround or patch available at time of publishing.	Microsoft Outlook Express XML File Attachment Script Execution	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
Microsoft [56]	Windows 98/ME/NT 4.0/2000, XP	Internet Explorer 6.0, Office Web Components 9, 10, Office XP	A vulnerability exists if an Internet Explorer user visits a specially designed web page, which could let a malicious user execute arbitrary programs.	No workaround or patch available at time of publishing.	Office XP/Internet Explorer	**High**	Bug discussed in newsgroups and websites.

[54] Bugtraq, August 5, 2002.
[55] NTBugtraq, July 27, 2002.
[56] Georgi Guninski Security Advisory #57, July 31, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Microsoft[57] ***Bulletin updated***[58]	**Windows 95/98/ME/NT 4.0/2000, XP**	**Windows Media Player XP, 6.4, 7.1**	**Several vulnerabilities exist: an information disclosure vulnerability exists due to the way the Windows Media Player handles certain types of licenses for secure media files when the media file is stored in the IE cache, which could let a malicious user execute arbitrary code; a privilege elevation vulnerability exists due to the way the Windows Media Device Manager Service handles requests to access local storage devices, which could let a malicious user obtain elevated privileges and take complete control over the machine; and a script execution vulnerability exists due to the way the Windows Media active playlist information is stored on the local system, which could let a malicious user execute arbitrary script code.** ***Bulletin revised to indicate a missing file from MS01-056 has been included. The omission has no effect on the effectiveness of the patch against the new vulnerabilities however, the original patch did not include all of the fixes discussed in Microsoft Security Bulletin MS01-056.***	**Frequently asked questions regarding this vulnerability and the patch can be found at:** **http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-032.asp** ***If you applied the patch delivered in Microsoft Security Bulletin MS01-056 and the one that was distributed with the original version of this bulletin, you're fully protected against all known vulnerabilities in Windows Media Player and don't need to take any action. Otherwise, we recommend that you apply the new version of the patch provided.***	**Windows Media Player Multiple Vulnerabilities** **CVE Names: CAN-2002-0372, CAN-2002-0373, CAN-2002-0615**	**High**	**Bug discussed in newsgroups and websites.** **Vulnerability has appeared in the press and other public media.**
Mozilla[59]	Unix	Mozilla Browser 1.0, 1.0 RC1&2, 1.1 Alpha	A Cross-Site Scripting vulnerability exists in the 'FTP View' feature due to improper sanitation, which could let a malicious user execute arbitrary JavaScript.	Upgrade available at: ftp://ftp.mozilla.org/pub/mozilla/releases/mozilla1.1b/	Mozilla 'FTP View' Cross-Site Scripting	High	Bug discussed in newsgroups and websites. Exploit has been published.

[57] Microsoft Security Bulletin, MS02-032, June 26, 2002.
[58] Microsoft Security Bulletin MS02-032 V2.0, July 24, 2002.
[59] SecurityFocus, August 6, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[60]	Unix	Cisco iSCSI Linux 2.1.2.1	A vulnerability exists in the configuration file because administrative credentials are stored in a world-readable file, which could let a malicious user obtain sensitive information. *Note: Installations of linux-iscsi installed from a distribution downloaded from Cisco or SourceForge are not vulnerable.*	No workaround or patch available at time of publishing.	iSCSI Insecure Configuration File	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
Multiple Vendors[61, 62, 63]	Unix	HP Secure OS software for Linux 1.0; Mandrake Soft Corporate Server 1.0.1, Mandrake 7.0, 7.1, 7.2, 8.0, 8.0 ppc, 8.1, 8.1 ia64, 8.2, Single Network Firewall 7.2; RedHat Linux 6.0, 6.0 sparc, alpha, 6.1, 6.1 sparc, alpha, 6.2, 6.2 sparc, alpha, 7.0, 7.0 alpha, 7.1, 7.1 ia64, alpha, 7.2, 7.2 ia64, alpha, 7.3; Sun Cobalt RaQ-RaQ 5, RaQ XTR, Cache RaQ series, Qube-Qube 3, Control Station	A vulnerability exists in the 'chfn' utility due to the failure to check the existence of a lockfile prior to performing sensitive operations, which could let a malicious user inject arbitrary data into these files to obtain elevated privileges.	**RedHat:** ftp://updates.redhat.com/ **Trustix:** http://www.trustix.net/pub/Trustix/updates/	Util-linux File Locking Race Condition CVE Name: CAN-2002-0638	Medium	Bug discussed in newsgroups and websites.

[60] iDEFENSE Security Advisory, 08.08.2002.
[61] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:132-14, July 29, 2002.
[62] Trustix Secure Linux Security Advisory, TSLSA-2002-0064, July 30, 2002.
[63] Hewlett-Packard Company Security, HPSBTL0207-054, July 30, 2002.

Vendor	**Operating System**	**Software Name**	**Vulnerability/ Impact**	**Patches/Workarounds/ Alerts**	**Common Name**	**Risk***	**Attacks/ Scripts**
Multiple Vendors[64, 65, 66, 67]	Unix	OSSP mm 1.0.0-1.0.12, 1.1.0-1.1.3	A vulnerability exists in the MM Shared Memory library due to the way temporary files are handled, which could let a malicious user obtain elevated privileges.	Upgrade available at: ftp://ftp.ossp.org/pkg/lib/mm/mm-1.2.1.tar.gz **Debian:** http://security.debian.org/pool/updates/main/m/mm/ **SuSE:** ftp://ftp.suse.com/pub/suse/ **Mandrake:** http://www.mandrakesecure.net/en/ftp.php **Slackware:** ftp://ftp.slackware.com/pub/slackware/slackware-current/patches/packages/apache-1.3.26-i386-2.tgz **RedHat:** ftp://updates.redhat.com/	MM Shared Memory Library Temporary File Privilege Escalation CVE Name: CAN-2002-0658	Medium	Bug discussed in newsgroups and websites.
Multiple Vendors[68, 69]	Unix	diet libc 0.18; GNU gcc 2.7.2, 2.95, 3.0. 3.1.1, glibc 2.0-2.0.6, 2.1-2.1.3, 2.1.9 & greater, 2.2-2.2.5, 2.3.10, glibc2 2.3.10, GNAT 3.14b	An integer overflow vulnerability exists during the computation of the memory region size by calloc and similar functions, which could let a malicious user obtain unauthorized root access to software linking to this code.	**diet libc:** http://www.fefe.de/dietlibc/dietlibc-0.19.tar.bz2 **Debian:** http://security.debian.org/pool/updates/main/d/dietlibc/ The GNU libc CVS repository contains a patch to add overflow detection to calloc.	Multiple Vendor calloc() Integer Overflow	**High**	Bug discussed in newsgroups and websites.

Multiple Vendors[70, 71]	Unix	FreeBSD 4.0-4.6, 4.1.1–4.6 STABLE, 4.1.1 - 4.3 RELEASE, 4.3 – 4.4 RELENG, 4.5 – 4.6 RELEASE;
		NetBSD 1.4.1-1.4.3, 1.5-1.5.3, 1.6 beta;
		OpenBSD 3.0, 3.1
			A vulnerability exists in some versions of the pppd daemon, which could let a malicious user change file permissions on arbitrary system files and obtain elevated privileges.	**FreeBSD:**
				ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-02:32/pppd.patch
				OpenBSD:
				ftp://ftp.openbsd.org/pub/OpenBSD/patches/
				NetBSD Advisory:
				http://www.NetBSD.ORG/Security/
					Multiple Vendor BSD pppd Arbitrary File Permission Modification	Medium	Bug discussed in newsgroups and websites.

[64] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:153-07, July 30, 2002.
[65] Mandrake Linux Security Update Advisory, MDKSA-2002:045, July 29, 2002.
[66] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:153-07, July 30, 2002.
[67] SuSE Security Announcement, SuSE-SA:2002:028, July 31, 2002.
[68] RUS-CERT Advisory 2002-08:02, August 5, 2002.
[69] Debian Security Advisory, DSA 146-1, August 8, 2002.
[70] FreeBSD Security Advisory, FreeBSD-SA-02:32, July 31, 2002.
[71] NetBSD Security Advisory 2002-010, August 2, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[72]	Windows 95/98/ME/NT 4.0/2000, XP, MacOS 9.0/ 9.0.4/ 9.1/ 9.2/ 9.2.1, MacOS X 10.x, Unix	Microsoft Internet Explorer 5.0, 5.0.1, 5.5, 5.5 SP1&2, 6.0; Mozilla Browser M16, M15, 0.8, 0.9.2-0.9.9, 1.0, 1.0 RC1&2, 1.1 Beta, 1.1 Alpha; Netscape Communicator 4.0, 4.5, 4.5 BETA, 4.6, 4.7, 4.51, 4.61, 4.72, 4.73, 4.74, 4.75, 4.76, 4.77, 4.78, 6.1, Netscape 6.0 1, 6.0 Mac, 6.0, 6.1, 6.2, 6.2.1, 6.2.2; Opera Software Opera Web Browser 5.0 2 win32, 5.0 Mac, 5.0 Linux, 5.1 1 win32, 5.1 0 win32, 5.12 win32, 5.12, 6.0 win32, 6.0, 6.0.1 win32, 6.0.1 Linux, 6.0.1, 6.0.2 win32, 6.0.3 win32	A vulnerability exists in the current specification of the JavaScript Same Origin Policy, which could let a malicious user retrieve content from and interact with any HTTP server behind the firewall.	**Microsoft:** Microsoft has investigated the issue and a fix has been included in IE 6 Service Pack 1, which is due to be released shortly. **Netscape:** Netscape/Mozilla has included a patch in the CVS repository [5].	Multiple Browser Vendor Same Origin Policy Design Error	Medium	Bug discussed in newsgroups and websites. Exploit has been published.

[72] XWT Foundation Security Advisory, July 29, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Multiple Vendors[73, 74, 75, 76, 77, 78, 79, 80]	MacOS X 10.x, Unix	Apple MacOS X 10.0-10.0.4, 10.1-10.1.5; FreeBSD 4.0-4.6, 4.1.1-4.6 STABLE, 4.1.1- 4.3 RELEASE, 4.3 - 4.4 RELENG, 4.5-4.6 – RELEASE; MIT Kerberos 5 1.0, 1.0.6, 1.1- 1.2.5; NetBSD 1.4-1.4.3, 1.5-1.5.3, 1.6; OpenBSD 2.0-3.1; Sun 2.5.1, 2.5.1_x86, _ppc, 2.6, 2.6 _x86, 2.7, 2.7 sparc, 2.8, 7.0, 7.0 _x86, 8.0, 8.0 _x86, 9.0; OpenAFS 1.0-1.0.4, 1.1-1.2.5, 1.3-1.3.2	A buffer overflow vulnerability exists in the xdr_array() procedure, which could let a remote malicious user execute arbitrary code and obtain unauthorized root access.	**Apple:** http://docs.info.apple.com/article.html?artnum=120139 **FreeBSD:** ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-02:34/rpc.patch **Debian:** http://security.debian.org/pool/updates/main/k/krb5/ **MIT Kerberos:** http://web.mit.edu/kerberos/www/advisories/2002-001-xdr_array_patch.txt **OpenBSD:** ftp://ftp.openbsd.org/pub/OpenBSD/patches/ **OpenAFS:** http://www.openafs.org/pages/security/xdr-updates-20020731.delta **NetBSD:** http://www.NetBSD.ORG/Security/	Multiple Vendor Sun RPC xdr_array Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.
Niels Chr Rød. Denmark[81]	Unix	Gender Mod 1.1.3	A SQL injection vulnerability exists which could let a remote malicious user subvert the SQL statement for updating profiles and obtain administrative access.	No workaround or patch available at time of publishing.	Gender Mod Administrative Access	**High**	Bug discussed in newsgroups and websites. Exploit has been published.

[73] Internet Security Systems Advisory, July 31, 2002.
[74] SGI Security Advisory, 20020801-01-A, August 1, 2002.
[75] FreeBSD Security Advisory, FreeBSD-SA-02:34 revised, August 1, 2002.
[76] NetBSD Security Advisory, 2002-011, August 2, 2002.
[77] Debian Security Advisory, DSA 142-1, August 5, 2002.
[78] Debian Security Advisory, DSA 143-1, August 5, 2002.
[79] OpenAFS Security Advisory, 2002-001, August 3, 2002.
[80] Apple Security Update, 2002-08-02, August 2, 2002.
[81] Bugtraq, July 27, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
NullSoft[82]	Windows 95/98/ME/NT 4.0/2000, XP	WinAmp 2.76, 2.79	A Cross-Site Scripting vulnerability exists because user supplied input in not properly sanitized before it is included when HTML playlists are generated, which could let a malicious user execute arbitrary script code.	No workaround or patch available at time of publishing.	WinAmp Playlist Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. There is no exploit code required.
NullSoft[83]	MacOS X, Unix	Shoutcast Server 1.8.9 Solaris, Mac OS X, Linux, FreeBSD	A vulnerability exists because administrative credentials are stored in a world-readable logfile, which could let a malicious user obtain sensitive information.	No workaround or patch available at time of publishing.	Shoutcast Insecure Permissions	Medium	Bug discussed in newsgroups and websites. There is no exploit code required.
OpenSSH[84]	MacOS X 10.x, Unix	OpenSSH 3.2.2 p1, 3.4 p1, 3.4	A Trojaned version of the OpenSSH package resides on ftp.openbas.org's server due to a recent compromise. A malicious user made modifications to the source code to include Trojan horse code. Downloads of the OpenSSH source code from ftp.openbsd.org between July 30, 2002 and July 31, 2002 likely contain the Trojan code, which could let a remote malicious user completely compromise the security of the server and execute arbitrary commands.	The vendor has fixed versions of openssh for download as of 1300 UTC August 1, 2002. They are available from the normal distribution channels and have the following MD5 checksums: ● MD5 (openssh-3.4p1.tar.gz) = 459c1d0262e939d6432f193c7a4ba8a8 ● MD5 (openssh-3.4p1.tar.gz.sig) = d5a956263287e7fd261528bb1962f24c ● MD5 (openssh-3.4.tgz) = 39659226ff5b0d16d0290b21f67c46f2 ● MD5 (openssh-3.2.2p1.tar.gz) = 9d3e1e31e8d6cdbfa3036cb183aa4a01 ● MD5 (openssh-3.2.2p1.tar.gz.sig) = be4f9ed8da1735efd770dc8fa2bb808a	OpenSSH Trojan Horse	**High**	Bug discussed in newsgroups and websites. Vulnerability has appeared in the press and other public media.

[82] Illegal Instruction Security Research Labs Advisory, August 4, 2002.
[83] Fate Research Laboratories Security Advisory, August 6, 2002.
[84] CERT® Advisory CA-2002-24, August 1, 2002. .

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
OpenSSL Project[85, 86, 87, 88, 89, 90, 91, 92, 93, 94]	Unix	OpenSSL 0.9.7 beta1&2	Multiple vulnerabilities exist: a buffer overflow vulnerability exists during the SSLv2 handshake process if a malformed key is used, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; a buffer overflow vulnerability exists during the SSLv3 handshake process if a large session ID is sent to the client during the handshake process, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; a buffer overflow vulnerability exists if Kerberos is enabled when a malformed key is sent during the SSLv3 handshake process, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; and multiple buffers overflow vulnerabilities exist in buffers that are used to hold ASCII representations of integers, which could let a remote malicious user cause a Denial of Service or execute arbitrary code.	Contact your vendor for current updates or see CERT® Advisory CA-2002-23 located at: http://www.cert.org/advisories/CA-2002-23.html **OpenSSL**: http://www.openssl.org/news/ **Debian:** http://security.debian.org/pool/updates/main/o/openssl/ **Trustix:** http://www.trustix.net/pub/Trustix/updates/ **Mandrake:** http://www.mandrakesecure.net/en/ftp.php **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **Caldera:** ftp://ftp.caldera.com/pub/security/OpenLinux/CSSA-2002-033.1.txt **Engarde:** http://ftp.engardelinux.org/pub/engarde/stable/updates/ **Oracle:** http://otn.oracle.com/deploy/security/htdocs/opensslAlert.html **Apple:** http://docs.info.apple.com/article.html?artnum=120139	Multiple OpenSSL Vulnerabilities CVE Name: CAN-2002-0655, CAN-2002-0656, CAN-2002-0657	Low/**High** **(High if arbitrary code can be executed)**	Bug discussed in newsgroups and websites. Exploit script has been published.

[85] CERT® Advisory CA-2002-23, July 30, 2002.
[86] Debian Security Advisory, DSA-136-1, July 30, 2002.
[87] Trustix Secure Linux Security Advisory, TSLSA-2002-0063, July 30, 2002.
[88] OpenPKG Security Advisory, OpenPKG-SA-2002.008, July 30, 2002.
[89] Gentoo Linux Security Announcement, July 30, 2002.
[90] Mandrake Linux Security Update Advisory, MDKSA-2002:046 1, August 6, 2002.
[91] SuSE Security Announcement, SuSE-SA:2002:027, July 30, 2002.
[92] Conectiva Linux Security Announcement, CLA-2002:513, July 31, 2002.
[93] Caldera International, Inc. Security Advisory, CSSA-2002-033.1, August 2, 2002.
[94] EnGarde Secure Linux Security Advisory, ESA-20020730-019, July 30, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
OpenSSL Project[95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107]	Windows NT 4.0, MacOS X 10.x, Unix	Apple MacOS X 10.0x; OpenSSL Project OpenSSL 0.9.1c, 0.9.2b, 0.9.3-0.9.7; Oracle Corporate Time Outlook Connector 3.1-3.1.2, 3.3, Oracle 9i Application Server 1.0.2.2, 1.0.2.1s, 1.0.2, Oracle HTTP Server 9.0.1, 9.2.0	A vulnerability exists in the ASN.1 library due to various encoding errors, which could allow malformed certificate encodings to be parsed incorrectly and cause a remote Denial of Service.	Users are strongly encouraged to upgrade existing versions of OpenSSL to version 0.9.6e or 0.9.7beta3. **Apple:** http://docs.info.apple.com/article.html?artnum=120139 **Debian:** http://security.debian.org/pool/updates/main/o/openssl/ **Mandrake:** http://www.mandrakesecure.net/en/ftp.php **RedHat:** ftp://updates.redhat.com/ **Slackware:** ftp://ftp.slackware.com/pub/slackware/slackware-current/patches/packages **Conectiva:** ftp://atualizacoes.conectiva.com.br/ **OpenBSD:** ftp://ftp.openbsd.org/pub/OpenBSD/patches/ **Trustix:** ftp://ftp.trustix.net/pub/Trustix/updates/ **Caldera:** ftp://ftp.caldera.com/pub/updates/OpenLinux/ **EnGarde:** http://ftp.engardelinux.org/pub/engarde/stable/updates/ **OpenPKG:** ftp://ftp.openpkg.org/release/1.0/UPD/openssl-0.9.6b-1.0.1.src.rpm	OpenSSL ASN.1 Parsing Error Denial of Service CVE Name: CAN-2002-0659	Low	Bug discussed in newsgroups and websites.

[95] CERT® Advisory CA-2002-23, July 30, 2002.
[96] Debian Security Advisory, DSA-136-1, July 30, 2002.
[97] Trustix Secure Linux Security Advisory, TSLSA-2002-0063, July 30, 2002.
[98] OpenPKG Security Advisory, OpenPKG-SA-2002.008, July 30, 2002.
[99] Gentoo Linux Security Announcement, July 30, 2002.
[100] Mandrake Linux Security Update Advisory, MDKSA-2002:046 1, August 6, 2002.
[101] SuSE Security Announcement, SuSE-SA:2002:027, July 30, 2002.
[102] Conectiva Linux Security Announcement, CLA-2002:513, July 31, 2002.
[103] Caldera International, Inc. Security Advisory, CSSA-2002-033.1, August 2, 2002.
[104] EnGarde Secure Linux Security Advisory, ESA-20020730-019, July 30, 2002.
[105] EnGarde Secure Linux Security Advisory, ESA-20020807-020, August 7, 2002.
[106] RedHat Security Advisory, RHSA-2002:160-21, August 5, 2002.
[107] Conectiva Linux Security Announcement, CLA-2002:516, August 8, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Opera Software[108]	Windows 95/98/ME/NT 4.0/2000, XP, Unix	Opera Web Browser 6.0, 6.0 win32, 6.0.1, 6.0.1 win32, 6.0.1 Linux, 6.0.2 win32-6.0.4 win32	A Cross-Site Scripting vulnerability exists because the data within <title> tags is not properly sanitized, which could let a malicious user execute arbitrary JavaScript.	No workaround or patch available at time of publishing.	Opera Cross-Site Scripting	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
ParaChat[109]	Multiple	ParaChat Server 4.0	A Denial of Service vulnerability exists when a user leaves the webpage where the room is located by using the Back or Forward buttons in place of the logoff button which leaves the account logged into the chat room.	Those affected by this vulnerability should contact the vendor regarding the availability of fixes.	ParaChat Denial of Service	Low	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Qual-comm, Inc.[110]	Windows 95/98/NT 4.0/2000	Eudora 5.1	A vulnerability exists because it is possible to refer to other files or attachments in a message through specially formatted inline text, which could let malicious attachments bypass normal warning dialogs.	No workaround or patch available at time of publishing.	Eudora File Attachment Spoofing	Medium	Bug discussed in newsgroups and websites. Exploit has been published.
Qual-comm, Inc.[111]	Windows 95/98/NT 4.0/2000	Eudora 5.0.2 -Jr2, 5.0.2, 5.1, 5.1.1	A buffer overflow vulnerability exists when a MIME multipart boundary message of arbitrary length is received, which could let a remote malicious user execute arbitrary code.	No workaround or patch available at time of publishing.	Eudora MIME Multipart Boundary Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.
Rob Flynn[112, 113, 114]	Unix	Gaim 0.56, 0.57	A buffer overflow vulnerability exists in the Jabber messaging plug-in module, which could let a remote malicious user execute arbitrary code.	**Rob Flynn:** http://prdownloads.sourceforge.net/gaim/gaim-0.59.tar.gz **RedHat:** ftp://updates.redhat.com/7.1/en/os/	Gaim Jabber Plug-In Buffer Overflow CVE Name: CAN-2002-0384	**High**	Bug discussed in newsgroups and websites.
Rod Clark[115]	Unix	Sendform versions 1.4.4 & prior	A Directory Traversal vulnerability exists by modifying the BlurbFilePath parameter, which could let a remote malicious user obtain sensitive information.	Upgrade available at: http://www.scn.org/~bb615/scripts/sendform.html	Sendform.cgi Directory Traversal CVE Name: CAN-2002-0710	Medium	Bug discussed in newsgroups and websites.

[108] Bugtraq, August 6, 2002.
[109] Bugtraq, July 31, 2002.
[110] Bugtraq, August 8, 2002.
[111] SNS Advisory No.55, August 8, 2002.
[112] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:107-11, August 5, 2002.
[113] Red Hat, Inc. Red Hat Security Advisory, RHSA-2002:098-14, August 5, 2002.
[114] Hewlett-Packard Company Security Advisory, HPSBTL0208-057, August 6, 2002.
[115] Bugtraq, July 30, 2002

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
SEH[116]	Multiple	IC9 7.1 .36, .30	A Denial of Service vulnerability exists when a malicious user sends an administrative password of 300 or more bytes.	No workaround or patch available at time of publishing.	SC9 Administrative Interface Password Denial Of Service	Low	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Sun Microsystems, Inc.[117]	Unix	Solaris 2.5.1, 2.6, 2.6 sparc, 7.0, 8.0	Buffer overflow vulnerabilities exist in the 'gfxres' and gxconfig' binaries, which could let a malicious user execute arbitrary code possibly with root privileges.	Patches available at: http://sunsolve.sun.com/pub-cgi/patchDownload.pl?target=107851&method=hs and http://sunsolve.sun.com/pub-cgi/patchDownload.pl?target=107714&method=h	Solaris GFXRES / PGXConfig Buffer Overflow	**High**	Bug discussed in newsgroups and websites.
Sun Microsystems, Inc.[118]	Unix	Answer Book2 1.2, 1.3.x, 1.4-1.4.2	A vulnerability exists because not all Admin scripts require authentication, which could let a remote malicious user perform administrative functions without an account and execute arbitrary code.	No workaround or patch available at time of publishing.	AnswerBook2 Unauthorized Administrative Script Access	**High**	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.
Sun Microsystems, Inc. / iPlanet[119]	Windows NT 4.0/2000, Unix	Sun ONE Web Server 4.1, 6.0; iPlanet E-Commerce Solutions iPlanet Web Server 4.x, 4.1, 4.1 SP1-9, 6.0, 6.0 SP1&2,	A vulnerability exists when processing requests coded with the 'Chunked Encoding' mechanism, which could let a remote malicious user execute arbitrary code.	**Sun One:** http://wwws.sun.com/software/download/download/5289.html	Sun ONE/iPlanet Web Server Chunked Encoding	**High**	Bug discussed in newsgroups and websites.

[116] Phenoelit Advisory, July 27, 2002.
[117] SecurityFocus, August 2, 2002.
[118] Bugtraq, August 1, 2002.
[119] eEye Digital Security Advisory, August 8, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
Symantec [120]	Windows 98/NT 4.0/2000, XP, Unix	Enterprise Firewall 6.5.2 NT/2000, 7.0 Solaris, 7.0 NT/2000, Gateway Security 5110, 5200, 5300, Ghost Corporate Edition 7.5, Raptor Firewall 6.5 Windows NT, 6.5.3 Solaris, Veloci Raptor 1.0, 1.1, 1.5	A vulnerability exists due to the way TCP Initial Sequence Numbers (ISNs) are created because the algorithm used for generating ISNs is not sufficiently random, which could let a remote malicious user hijack any connection or traverse the Raptor Firewall.	Updates available at: ftp://ftp.symantec.com/public/updates/	Multiple Symantec Product Weak TCP Initial Sequence Numbers Randomization	Medium	Bug discussed in newsgroups and websites.
Synthetic Reality[121]	Unix	Sympoll 1.2	A vulnerability exists if the 'register_globals' directive is enabled due to a insufficient integrity checking of variables, which could let a remote malicious user obtain sensitive information.	Upgrade available at: http://www.ralusp.net/downloads/sympoll/sympoll.tar.gz	Sympoll File Disclosure	Medium	Bug discussed in newsgroups and websites. Vulnerability can be exploited via a web browser.

[120] Ubizen Security Advisory, August 2, 2002.

[121] Bugtraq, July 30, 2002.

Vendor	Operating System	Software Name	Vulnerability/ Impact	Patches/Workarounds/ Alerts	Common Name	Risk*	Attacks/ Scripts
T. Hauck[122]	Windows 95/98/ME/NT 4.0/2000	Jana WebServer 1.0, 1.45, 1.46, 2.0, 2.0 Beta 1&2, 2.2.1	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the HTTP proxy server and HTTP server when an extremely long HTTP request is sent, which could let a malicious user cause a Denial of Service; a buffer overflow vulnerability exists in the SOCKS5 proxy server when a username, password or hostname that are longer than 127 characters is authenticated; a buffer overflow vulnerability exists in the POP3 gateway service when a malicious server returns an oversized reply to the Jana server; a buffer overflow vulnerability exists in the SMTP gateway service, which could let a malicious server return an oversized replay to the Jana Server and cause a Denial of Service; a vulnerability exists because the FTP PASV command server allocates a TCP port without closing the previously allocated port, which could let a remote malicious user cause a Denial of Service; a vulnerability exists because different diagnostics are given for valid and invalid usernames and an unlimited number of authentication attempts are allowed which could let a malicious user bruteforce the username/password; and a vulnerability exists in the POP3 array index because POP3 message index values are not properly validated, which could let a malicious user cause a Denial of Service.	No workaround or patch available at time of publishing.	Jana WebServer Multiple Vulnerabilities	Low/ Medium (Medium if sensitive information is obtained)	Bug discussed in newsgroups and websites.
William Deich[123]	Unix	Super 3.12, 3.16-3.18	A format string vulnerability exists due to the incorrect use of the syslog() function to log error messages, which could let a malicious user obtain unauthorized root access.	**Debian:** http://security.debian.org/pool/updates/main/s/super/ **William Deich:** ftp://ftp.ucolick.org/pub/users/will/super-3.19.0.tar.gz	Super SysLog Format String	**High**	Bug discussed in newsgroups and websites. Exploit script has been published.

[122] SECURITY.NNOV Notification, July 26, 2002.
[123] Debian Security Advisory, DSA 139-1, August 1, 2002.

*"Risk" is defined by CyberNotes in the following manner:

High - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.

Medium – A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.

Low - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. *DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.*

Recent Exploit Scripts/Techniques

The table below contains a representative sample of exploit scripts and How to Guides, identified between July 29 and August 8, 2002, listed by date of script, script names, script description, and comments. **Items listed in boldface/red (if any) are attack scripts/techniques for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that malicious users are utilizing**. During this period, 21 scripts, programs, and net-news messages containing holes or exploits were identified. *Note: At times, scripts/techniques may contain names or content that may be considered offensive.*

Date of Script (Reverse Chronological Order)	Script Name	Script Description
August 8, 2002	**Eudora-exp.pl**	**Perl script which exploits the Eudora MIME Multipart Boundary Buffer Overflow vulnerability.**
August 8, 2002	Lsrscan-0.2.tar.gz	A scanner that will determine whether remote hosts will return source routed connections, or forward source routed packets to a remote host.
August 8, 2002	Lsrtunnel-0.2.tar.gz	Lsrtunnel spoofs connections to a remote host by pretending to be the middle host in a source routed path.
August 7, 2002	Arp-sk-0.0.12.tgz	An ARP packet generator for Unix designed to illustrate ARP protocol flaws and applications such as ARP cache poisoning. or MAC spoofing. It gives complete control of link and network level data.
August 6, 2002	**Mssql_hello_overflow.nasl**	**Exploit for the SQL Server Remote Buffer Overflow vulnerability.**
August 6, 2002	**Qmailadmin-exp.c**	**Script which exploits the qmailadmin Buffer Overflow vulnerability.**
August 6, 2002	**Shatter.zip**	**Exploit for the Microsoft Windows Window Message Subsystem Design Error vulnerability**
August 6, 2002	SPIKE2.5.tar.gz	An easy to use generic protocol API that helps reverse engineer new and unknown network protocols that features several working examples.
August 5, 2002	Nmap-3.00.tgz	A utility for port scanning large networks.
August 5, 2002	**Sicillian.pl**	**Perl script which exploits the Trillian Buffer Overflow vulnerabilities.**
August 1, 2002	Tw-imap.c	Script which exploits the remote IMAP4rev1(lsub) vulnerability.

Date of Script (Reverse Chronological Order)	Script Name	Script Description
July 31, 2002	GOBBLES-own-super.c	Script which exploits the Super SysLog Format String vulnerability.
July 31, 2002	Nessus-1.2.3.tar.gz	An up-to-date, and full featured remote security scanner for Linux, BSD, Solaris and some other systems that is multithreaded, plugin-based, has a nice GTK interface, and currently performs over 910 remote security checks.
July 31, 2002	Opensslrv.txt	Exploit for the Multiple OpenSSL Vulnerabilities.
July 30, 2002	Eat_gopher.pl	Perl script which exploits the IE gopher buffer overflow vulnerability.
July 30, 2002	**Imailexp.c**	**Script which exploits the IMail Web Calendaring Denial of Service vulnerability.**
July 30, 2002	Su.c	Script which exploits the Tru64 SU Buffer Overflow vulnerability.
July 30, 2002	**Tcptraceroute-1.4.tar.gz**	**An implementation of traceroute which uses TCP SYN packets, instead of the more traditional UDP or ICMP ECHO packets. and is able to trace through many common firewall filters.**
July 30, 2002	Xploit.phps	PHP exploit lab v1.0 that attempts to browse, read, execute, and mysqlread.
July 30, 2002	Xss-faq.txt	The Cross Site Scripting FAQ includes threat analysis, examples of cross site scripting attacks, cookie theft, how to protect yourself, and how to fix the holes.
July 29, 2002	Lameident3-exp.c	Script which exploits the Fake Identd Client Query Remote Buffer Overflow vulnerability.

Trends

- **The National Infrastructure Protection Center (NIPC) has issued an advisory to heighten the awareness of multiple buffer overflows in OpenSSL (Open Secure Sockets Layer). For more information, see "Bugs, Holes & Patches" Table and NIPC Advisory 02-006, located at: http://www.nipc.gov/warnings/advisories/2002/02-006.htm.**
- **There has been an increase in scanning for the Apache Chunk Encoding Vulnerability and direct reports of exploitation have been received by CERT/CC. For more information see** http://www.cert.org/current/current_activity.html#Apache**.**
- **A warning has been issued by NIPC regarding a potential vulnerability in numerous versions of the open-source Apache Web Server Software. This vulnerability can allow remote access to the system and gives an intruder the ability to take control of the system and execute root level commands. NIPC considers this to be a significant threat due to the large installed base of Apache Servers, the potential for remote compromise, and the level of access granted by this vulnerability. For more information, see NIPC Advisory 02-005, located at: http://www.nipc.gov/warnings/advisories/2002/02-005.1.htm**
- **BSD/Scalper.worm is an Internet Worm that spreads over Apache web servers on FreeBSD by using the Chunked Encoding exploit.**
- **Numerous exploit scripts exist which exploit the Apache Chunked-Encoding Memory Corruption vulnerability.**

Viruses

The following virus descriptions encompass new viruses and variations of previously encountered viruses that have been discovered in the last two weeks. The viruses are listed alphabetically by their common name. While these viruses might not all be in wide circulation, it is highly recommended that users update anti-virus programs as often as updates become available. *NOTE: At times, viruses may contain names or content that may be considered offensive.*

BAT_ETIMOLOD.A (Batch File Virus): This destructive batch file virus drops various copies of itself in the following directories:

- C:\
- C:\Windows\System
- C:\Windows\System32
- C:\Windows\Start Menu

It also deletes critical system files on the target machine.

BAT_KRAZYB.A (Alias: BAT.Krazyb.A@mm) (Batch File Virus): This mass-mailing worm, created in a batch file, propagates through Microsoft Outlook. It sends copies of itself to all addresses listed in the contact list with the following e-mail characteristics:

- Subject: Hi!
- Message Body: Here's a great game for all ages.IT's called blackjackel.Have a nice day :)
- Attachment:c:\KrAzY_BoI.bat

The worm can also propagate via mIRC and has a destructive payload of deleting certain Antivirus system files.

IRC/Gleep (Internet Worm): This is an Internet worm that attempts to send itself to others using mIRC and KaZaa. When this virus is activated on a host system, it will modify the MIRC.INI file with instructions to load a newly created SCRIPT.INI. The SCRIPT.INI file contains instructions to connect to the IRC network using an IRC server named irc.megatokyo.com, and join a channel named "mtartanddrawing." This message is sent to the channel:

- Gleep is a Biznatch and w3r3z tha b33f

A message is also sent to a mIRC user (possibly the author) with this note:

- gleep.bug--

Next, the SCRIPT.INI instructs mIRC to join the channel "akufansubs" and send a note to others suggesting trading pictures. An attempt is then made to send a file "C:\My_Self_picture.zip" to other users. Due to bugs in the code, this file is never created. The script screens for the string "pic" and if this string is identified, the infected system will attempt to send the file "C:\My_Self_picture.jpg.exe." Due to bugs in the code, this file is never created. IRC/Gleep will also attempt to delete the following files from the infected host:

- cdplayer.exe
- defrag.exe
- edit.com
- notepad.exe
- pbrush.exe
- welcome.exe
- winfile.exe

IRC.Mizi.Worm (Alias: IRC/Muzik) (Internet Worm): This is an IRC worm that spreads by using mIRC to send messages to people who join a channel to which the current host is connected. The worm attempts to persuade the person who received the message to download a copy of the worm from an Internet site. This worm can no longer spread because the site that contained the copy of the worm no longer exists (since before July 30, 2002).

VBS/Galla@MM (Visual Basic Script Worm): This mass mailing worm attempts to send itself to all recipients found in the Microsoft Outlook Address Book. It arrives in an e-mail message using the following information:

- Subject: RV:Congreso de seguridad eGallaecia'02 (http://www.e-gallaecia.com)
- Body: He recibido esta info, creo que te va a interesar.
- Attachment: XXXX.VBS (where XXXX is a random filename).

Which translates to:

- Subject: RV: Congress of security eGallaecia'02(http://www.e-gallaecia.com)
- Body: I have received this info, I think it would interest you.

VBS/Lubus.C (Visual Basic Script Worm): This is a worm that uses e-mail to spread. The message that carries this worm is very easy to recognize as its subject is always TH and the name of the attached file is THWIN.VBS. The actions that VBS/Lubus.C carries out includes eliminating files with certain extensions, as well as dropping another worm, called VBS/Redlof.A, to the system and running it. Every time it is run, VBS/Lubus.C deletes five randomly selected files from those that have one of the following extensions: XLS, DOC, WAV, DWG, MP3, BAK, WAV, BMP, HTM, HLP, CHM, JPG, GIF, SCR, TTF, MID, CDR, MDB, DBF and ICO.

VBS_NIEBER.A (Aliases: NIEBER.A, Bernie, VBS.Neiber.A@mm) (Visual Basic Script Worm): This mass-mailing worm arrives in an e-mail message with the following:

- Subject: Attention virus

Upon execution, this worm copies itself to the BERNIE.VBS file in the %System% directory. Then, it adds this registry key so that its dropped file executes upon system startup:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\ CurrentVersion\Run Bernie = “wscript.exe %System%\Bernie.vbs”

Next, it checks for the existence of this registry key:

- HKEY_CURRENT_USER\software\Bernie\mailed

If it does not find the registry key, it sends out an HTML formatted e-mail, which contains the viral codes of this worm. It uses Microsoft Outlook to send the infected e-mail to all the addresses listed in the infected system's Windows Address Book (WAB). Then it creates and sets this registry key to 1, to mark the execution of its mass-mailing on the infected system:

- HKEY_CURRENT_USER\software\Bernie\mailed

It also searches all local or mapped drives, folders, and subfolders for files with these extension names and then overwrites these with its copy: .VBE, and .VBS. It runs several Notepad applications until all system resources are exhausted. No other application can be opened or run after this because Windows runs out of free memory. It also modifies the Start Page of the infected system's Internet Explorer with the following registry entries:

- HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main Start Page = "http:\\membres.lycos.fr\aoteam\mange.com"

VBS_PICA.N (Visual Basic Script Worm): This Visual Basic Script mass-mailing worm spreads via Microsoft Outlook, mIRC, PIRCH, and through local networks. It sends e-mail with the following details to all recipients in the Microsoft Outlook address book:

- Subject: “Here you have, ;o)”
- Message Body: “Hi!” “Check this!”
- Attachment: Sysboot.dll.vbs

VBS_SEALUG.A (Alias: VBS.Sealug@mm) (Visual Basic Script Worm): This is a mass-mailing worm that is created in Visual Basic Script. It propagates through Microsoft Outlook with the following e-mail characteristics:

- Subject: En SevdiginMessage
- Body: Hayat yasandigi kadardir. Ötesi ya hatiralarda bir iz, ya da hayallerde bir umuttur. Hüsrani ise bir tek yerde kabul edebilirim: O da yasamaya olanak varken yasayamamis olmaktir.
- Attachment: En_Sevdigin.vbs

W32.Assarm@mm (Aliases: WORM_ASSARM.A, ASSARM.A) (Win32 Worm): This is a mass-mailing worm that sends messages in reply to all unread messages in the Microsoft Outlook Mailbox. The e-mail messages are not sent if the day of the week is Monday or Thursday, and the hour of the time of day is greater than five. The subject of the e-mail message is "Re: <original message subject line>" and the attachment varies.

W32.AJM.Worm (Win32 Worm): This is a mass-mailing worm. It uses Microsoft Outlook to send itself to e-mail addresses that it retrieves from all unread e-mail messages. The subject line and message body of the e-mail are written in Korean. The attachment file name may also contain Korean characters. The following are some attachment names:

- Heddink.exe
- Go Korea.exe
- RedDevil.exe
- WorldCup.exe
- 2002.exe

W32.BleBla.J.Worm (Win32 Worm): This is a variant of W32.Blebla.B.Worm. It arrives as an e-mail message that has an HTML body and two attachments: Melh32.exe and Melhw32.chm. When you read the message, the two attachments are automatically saved and launched. The worm then attempts to send itself to all contacts in the Microsoft Outlook Address Book and post messages to a newsgroup. The worm also alters registry keys so that it runs when certain types of files are viewed or executed.

W32/Chir-B (Aliases: Win32/ChiHack, WORM_CHIR.B, I-Worm.Runouce.b, PE_CHIR.B, W32.Chir.B@mm) (Win32 Worm): This is an e-mail worm, an EXE file infector, and an HTM/HTML file infector. The worm component attempts to spread via e-mail by sending itself to e-mail addresses found in the Windows address book, plus addresses found in files matching *.adc, *r.db, *.doc, and *.xls. The e-mail will have the following characteristics:

- From: <username>@yahoo.com or imissyou@btamail.net.cn
- Subject line: <username> is coming!
- Attached file: Name of infected file.

The body of the e-mail will be blank. The e-mail contains the Iframe exploit and a MIME exploit to run the virus automatically when the e-mail is viewed. When run, the virus will copy itself into the Windows system folder as runouce.exe and sets the following registry entry to point to this new copy of the virus:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Runonce

This will cause the virus to be started when Windows starts up. The virus continually monitors this registry entry so that any attempt to change or delete the entry will result in the entry being reset with the value described above. It searches for HTM and HTML files on both the local system and network drives. If files of this type are found in a folder, then a file named readme.eml is created in that folder and a line of HTML code is appended to the HTM and HTML files. This HTML code contains a short JavaScript component that is intended to open the file, readme.eml. Readme.eml contains a base64 encoded copy of the virus. A second EML file with the same contents as readme.eml may also appear in folders on network drives. This file will have the filename <computername>.eml. The virus also infects Windows executables on both local and network drives but will not infect files in folders matching "wind*" or "winn*," including all subfolders of those folders. This means that files in folders with names such as Windows or Winnt will not be infected. On the first of the month, W32/Chir-B will overwrite the first 1234 bytes of files matching *.adc, *r.db, *.doc and *.xls with garbage. W32/Chir-B employs a technique that will cause the virus to be restarted if its process is terminated.

W32/EnerKaz.worm.b (Win32 Worm): This worm spreads via the KaZaa peer-to-peer file-sharing network. It requires the KaZaa software to be running to propagate, and requires that at least 98 different local content folders are being shared. When run, the worm displays a message box. It creates the folder %WinDir%\Sys32 and copies itself there as spank_britney.exe. It then modified the KaZaa sharing folder to point to the newly created one. This is accomplished through a registry key:

- HKEY_CURRENT_USER\Software\Kazaa\LocalContent\dir99=012345:C:\WINDOWS\sys32

An additional key is created to assure that KaZaa's sharing setting is enabled:

- HKEY_CURRENT_USER\Software\KAZAA\LocalContent\DisableSharing=0

W32.Golsys.8020 (Win32 Virus): This is a multi-threaded worm that is written in assembly language. When executed, it creates the file %system%\Sysl0gon.exe. The virus will also attempt to infect all executable files that it can find, both on the local hard drive and on mapped drives.

W32.HLLW.Lama (Win32 Worm): This is a mass-mailing worm that uses Microsoft Outlook to send itself to all contacts in the Microsoft Outlook Address Book. It can also spread by mIRC and KaZaa shared folders. The e-mail has numerous possible subjects, messages, and attachments.

W32.HLLW.Yoohoo (Aliases: W32.HLLW.Spear, W32.HLLW.Yoohoo.B) (Win32 Worm): This is a worm that copies itself to the shared folders of KaZaa, Bearshare, Morpheus, and eDonkey2000. It is written is Borland Delphi programming language and may be compressed with UPX.

W32.Langex@mm (Win32 Worm): This mass-mailing worm uses MAPI to replicate. The subject of the e-mail is variable as the worm simply replies to e-mails it finds on an infected system. The name of the attachment is "lang.exe." This worm contains no payload.

W32/Lohack.c@MM (Aliases: W32/Lohack.gen@MM**, Win32.HLLM.Gdies.45056, Win32.Lohack.C) (Win32 Worm):** This is a mass-mailing worm that also spreads via the KaZaa file-sharing network. It is a UPX packed Microsoft Visual C++ executable and arrives in an e-mail message containing the following information:

- Subject: Windows update
- Body: Install this Windows update (for all versions)
  http://www.[omitted].hpg.com.br/update.html
- Attachment: windows_update.txt.exe

Running the attachment causes the worm to send itself, using MAPI, to e-mail addresses found in.DBX, .EML, .HTM, .IDX, .MDX, .MSG, .NCH, and .TXT files found on the system. If the user does not run the attachment, but does visit the link in the e-mail message, script on the page will attempt to refresh and load an e-mail file "update.eml." The e-mail file contains an IFrame exploit that may launch an embedded copy of "windows_update.txt.exe." This virus will also copy itself to the default shared folder location for KaZaa, a peer-to-peer (P2P) file sharing client application, with a duplicate file name with a .URL extension as a hyperlink to the web location of the virus. The typical default shared folder is: C:\Program Files\KaZaA\My Shared Folder\.

W32/Onamu-B (Aliases: WORM_MOE.B, I-Worm.Desos.b) (Win32 Worm): This worm has been reported in the wild. It spreads via SMTP and arrives as an attachment to an e-mail. The e-mail appears to come from a fake name and e-mail address selected from random names and addresses. It will also contain various subject lines, message text and attachments. The worm copies itself to the Windows folder with a filename consisting of five randomly chosen letter and an EXE extension and adds a registry entry to:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run

so that the worm is run when Windows starts.

W32/Surnova-B (Win32 Worm): This worm has been reported in the wild. It spreads using the KaZaa network software installation and the MSN instant messenger utility. The worm will initially copy itself to the Windows folder with various filenames. W32/Surnova-B sets the following registry entry to point to the new copy of the worm so that the file is run when Windows starts up:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\Supernova

When first executed, the worm displays the fake error message "Application attempted to read memory at 0xFFFFFFFFh Terminating application." It searches the following registry entry for a folder that is shared across the KaZaa network:

- HKLM\Software\KaZaA\LocalContent

If a value is not found, then the folder C:\<Windows>\Media is used. The worm creates thirty eight copies of itself in this folder with various filenames. W32/Surnova-B will also attempt to send itself to contacts in the infected user's Messenger contact list. The worm will arrive with one of the following messages:

- Hehe, check this out :-)
- Funny, check it out (h)
- LOL!! See this :D
- LOL!! Check this out :)Hehe, this is fun :-)

The worm creates a text file in the Windows folder with a name consisting of randomly generated digits. The text file contains the text:

- W32.Supernova - Ban religion
- Patch the leaks or the ship will sink

W97M.Alarm (Word 97 Macro Virus): This is a Microsoft Word macro virus that infects active documents and the global template, Normal.dot. This macro virus has a payload to replace some of the C:\Windows\System files with spaces and some garbage bytes.

W97M.Bablas.AT (Word 97 Macro Virus): This is a Microsoft Word macro virus that infects active documents and the global template, Normal.dot. The name of the module it uses to infect with is "GUINDA." This virus also disables access to the Macro Editor and changes the captions of the menu. W97M.Bablas.AT also creates the file C:\Guindalo.vxd. This file contains a text message.

W97M/Opey.bd (Word 97 Macro Virus): The virus will disable the macro warning for Word97. It contains two modules - Linis_Cls and Linis_Bbq. The virus does not contain malicious code.

W97M.Peddec.A (Word 97 MacroVirus): This is a Microsoft Word macro virus that infects Word documents when you open them. The virus also disables many functions that are used to view the source code of the Word macro.

W97M.Twopey.C (Word 97 Macro Virus): This is a macro virus that infects Microsoft Word documents and templates. The properties of infected documents may be configured as follows:

- Author: OPEY A." 'GREETINGS TO ALL FILIPINO PROGRAMMERS !!!
- Title: OpeY 2k1 version - Philippines

The virus writes its source code to the System.txt file, which is a temporary file in the startup path for Microsoft Office. This file is removed after infection.

WORM_BIHUP.A (Internet Worm): This is a mass-mailing worm that sends itself to addresses found in unread e-mail messages of Outlook Express. The subject and message body of the infected e-mail are written in Korean language. The attachment may be any of the following:

- Heddink.exe
- Go Korea.exe
- RedDevil.exe
- WorldCup.exe
- 2002.exe

WORM_GDIES.A (Internet Worm): This worm propagates via the KaZaa file sharing network and via e-mail using Microsoft Outlook. It sends the following e-mail with a copy of itself as attachment:

- Subject: Windows update
- Message Body: Install this Windows update (for all versions).
- Attachment: windows_update.txt.exe

The file attachment on this e-mail message automatically executes on systems running unpatched Internet Explorer 5.01 and 5.5.

WORM_KWBOT.B (Internet Worm): This Internet worm propagates via KaZaa, a peer-to-peer file sharing utility. It facilitates remote access and manipulation by malicious users. It is a variant of the WORM_KWBOT.A.

WORM_SAMBUD.A (Aliases: W32/EnerKaz.worm, Worm.P2P.Sambud, W32.HLLW.Sambut, Win32/Fork.Worm, W32/EnerKaz.worm.a) (Internet Worm): This memory-resident worm propagates via KaZaa, the popular file-sharing application. It drops a copy of itself in its created folder named SYS32, inside the Windows folder. This worm displays either a blank message box or one that contains the following text strings:

- You are a DUMB ASS!!:)MWHAHAHAH

Worm/Singapore (Internet Worm): This is an Internet worm that spreads through e-mail by using addresses it collects in the Microsoft Outlook Address Book, as well as, through the use of the Internet Rely Chat (IRC) network. The worm arrives through e-mail in the following format:

- Subject: Happy National Day Singapore!
- Body: Happy Birthday To Singaporeans!!!
- Attachment: NationalDay2002.vbs

If executed, the worm copies itself in the directory under which it is run using the filename "national.bat." It then copies itself the root directory (C:\) under the file names "NationalDay2002.bat" and "NationalDay2002.vbs." Once the spreading routine is finished, these files are then deleted. Additionally, the file "system.ini" file gets modified. Various files are created in the \windows\ directory. So that it can spread through IRC, the following file gets modified, "script.ini." It will also try to delete various antivirus software applications, including "avp32.exe, antivir.vdf, tc.exe, scan.dat, tbav.dat, fpw32.dll, and various Norton applications." Worm/Singapore contains the following text:

- Singapore 37th Birthday!! Happy National Day To All Of You
- This worm is done to celebrate Singapore National Day!! By SGBoy
- I love Singapore, don't you?

WORM_SURNOVA.C (Aliases: Worm.P2P.Surnova.C, Win32.Supova) (Internet Worm): This worm is a variant of WORM_SURNOVA.B. It propagates via MSN Messenger and KaZaa, a peer-to-peer application, which enables users to share files over a network.

WORM_SURNOVA.F (Alias: Worm.P2P.Surnova.f) (Internet Worm): This memory-resident worm drops several copies of itself in either the KaZaa file-sharing folder or the Windows Media folder. It propagates copies of itself using MSN Messenger and the KaZaa peer-to-peer (P2P) application.

WORM_SURNOVA.G (Internet Worm): This memory–resident worm drops several copies of itself in either the shared KaZaa or Windows Media folder. It propagates copies of itself via the KaZaa peer-to-peer (P2P) application.

WORM_SYTRO.C (Aliases: W32.HLLW.Kazmor.C, Worm.P2P.Sytro.c, W32/Qtint.worm.c) (Internet Worm): This worm propagates via the Morpheus file-sharing network. It disguises itself as movie files, games, or pornographic materials.

XM97/Anis-D (Excel 97 Macro Virus): Unlike many Excel macro viruses, XM97/Anis-D does not create an infected file in the XLSTART directory. This virus copies itself directly from one open file to another.

XM.Laroux.ST (Excel Macro Virus): This Microsoft Excel macro virus is a variant of XM.Laroux. It creates the file Personal.xls in the Excel Startup folder. It then uses this file to infect Excel spreadsheets. This macro virus has a module named "birth" that it uses to infect other Excel files.

Trojans

Trojans have become increasingly popular as a means of obtaining unauthorized access to computer systems. This table includes Trojans discussed in the last six months, with new items added on a cumulative basis. Trojans that are covered in the current issue of CyberNotes are listed in boldface/red. Following this table are write-ups of new Trojans and updated versions discovered in the last two weeks. Readers should contact their anti-virus vendors to obtain specific information on Trojans and Trojan variants that anti-virus software detects. *Note: At times, Trojans may contain names or content that may be considered offensive.*

Trojan	Version	CyberNotes Issue #
AIM-Flood	**N/A**	**Current Issue**
APStrojan.sl	N/A	CyberNotes-2002-03
Arial	N/A	CyberNotes-2002-08

Trojan	Version	CyberNotes Issue #
Backdoor.Anakha	N/A	CyberNotes-2002-13
Backdoor.AntiLam	N/A	CyberNotes-2002-12
Backdoor.Assasin	N/A	CyberNotes-2002-14
Backdoor.Crat	N/A	CyberNotes-2002-12
Backdoor.Delf	**N/A**	**Current Issue**
Backdoor.Delf.B	**N/A**	**Current Issue**
Backdoor.Ducktoy	N/A	CyberNotes-2002-15
Backdoor.Easyserv	**N/A**	**Current Issue**
Backdoor.EggHead	N/A	CyberNotes-2002-04
Backdoor.Evilbot	N/A	CyberNotes-2002-09
Backdoor.Fearic	**N/A**	**Current Issue**
Backdoor.FTP_Bmail	N/A	CyberNotes-2002-12
Backdoor.G_Door.Client	N/A	CyberNotes-2002-05
Backdoor.GRM	N/A	CyberNotes-2002-13
Backdoor.GSpot	N/A	CyberNotes-2002-12
Backdoor.IISCrack.dll	N/A	CyberNotes-2002-04
Backdoor.Kavar	**N/A**	**Current Issue**
Backdoor.Latinus	N/A	CyberNotes-2002-12
Backdoor.Mirab	N/A	CyberNotes-2002-13
Backdoor.MLink	**N/A**	**Current Issue**
Backdoor.NetControle	N/A	CyberNotes-2002-13
Backdoor.NetDevil	N/A	CyberNotes-2002-04
Backdoor.Nota	N/A	CyberNotes-2002-12
Backdoor.Omed.B	N/A	CyberNotes-2002-11
Backdoor.RemoteNC	N/A	CyberNotes-2002-09
Backdoor.Sazo	N/A	CyberNotes-2002-13
Backdoor.Sparta	N/A	CyberNotes-2002-13
Backdoor.Subwoofer	N/A	CyberNotes-2002-04
Backdoor.Surgeon	N/A	CyberNotes-2002-04
Backdoor.Systsec	N/A	CyberNotes-2002-04
Backdoor.Theef	N/A	CyberNotes-2002-15
Backdoor.Tron	N/A	CyberNotes-2002-12
Backdoor.Ultor	N/A	CyberNotes-2002-13
Backdoor.WinShell	**N/A**	**Current Issue**
BackDoor-ABH	N/A	CyberNotes-2002-06
BackDoor-ABN	N/A	CyberNotes-2002-06
BackDoor-FB.svr.gen	N/A	CyberNotes-2002-03
Banan.Trojan	N/A	CyberNotes-2002-15
Bck/Litmus.201	N/A	CyberNotes-2002-14
BDS/ConLoader	N/A	CyberNotes-2002-12
BDS/Osiris	N/A	CyberNotes-2002-06
BKDR_EMULBOX.A	N/A	CyberNotes-2002-10
BKDR_INTRUZZO.A	N/A	CyberNotes-2002-09
BKDR_LITMUS.C	N/A	CyberNotes-2002-09
BKDR_SMALLFEG.A	N/A	CyberNotes-2002-04

Trojan	Version	CyberNotes Issue #
BKDR_WARHOME.A	N/A	CyberNotes-2002-06
Dewin	N/A	CyberNotes-2002-08
DoS-Winlock	N/A	CyberNotes-2002-03
Downloader-W	N/A	CyberNotes-2002-08
FakeGina.Trojan	**N/A**	**Current Issue**
Fortnight	N/A	CyberNotes-2002-10
IRC.kierz	**N/A**	**Current Issue**
Irc-Smallfeg	N/A	CyberNotes-2002-03
IRC-Smev	N/A	CyberNotes-2002-08
JS/NoClose	N/A	CyberNotes-2002-11
Liquid.Trojan	N/A	CyberNotes-2002-14
mIRC/Gif	N/A	CyberNotes-2002-08
Multidropper-CX	N/A	CyberNotes-2002-08
PWS-AOLFake	N/A	CyberNotes-2002-15
PWS-Ritter	**N/A**	**Current Issue**
QDel227	N/A	CyberNotes-2002-09
QDel234	N/A	CyberNotes-2002-11
RCServ	N/A	CyberNotes-2002-10
StartPage-B	**N/A**	**Current Issue**
Swporta.Trojan	N/A	CyberNotes-2002-13
TR/Win32.Rewin	N/A	CyberNotes-2002-12
Tr/WiNet	N/A	CyberNotes-2002-10
TR/Zirko	N/A	CyberNotes-2002-10
Troj/Diablo	N/A	CyberNotes-2002-09
Troj/DSS-A	N/A	CyberNotes-2002-12
Troj/Flood-O	N/A	CyberNotes-2002-14
Troj/ICQBomb-A	N/A	CyberNotes-2002-05
Troj/Kbman	N/A	CyberNotes-2002-10
Troj/Momma-B	N/A	CyberNotes-2002-11
Troj/Msstake-A	N/A	CyberNotes-2002-03
Troj/Tobizan-A	**N/A**	**Current Issue**
Troj/Unreal-A	**N/A**	**Current Issue**
TROJ_DOAL.A	N/A	CyberNotes-2002-14
TROJ_DSNX.A	N/A	CyberNotes-2002-03
TROJ_ICONLIB.A	N/A	CyberNotes-2002-03
TROJ_JUNTADOR.B	N/A	CyberNotes-2002-06
TROJ_JUNTADOR.G	N/A	CyberNotes-2002-10
TROJ_OPENME.B	N/A	CyberNotes-2002-09
TROJ_SMALL.J	N/A	CyberNotes-2002-10
TROJ_SMALLFEG.DR	N/A	CyberNotes-2002-04
TROJ_SQLSPIDA.B	N/A	CyberNotes-2002-11
TROJ_WORTRON.10B	N/A	CyberNotes-2002-12
Trojan.Allclicks.A	N/A	CyberNotes-2002-13
Trojan.Beway	N/A	CyberNotes-2002-15
Trojan.Fatkill	N/A	CyberNotes-2002-09

Trojan	Version	CyberNotes Issue #
Trojan.Junnan	**N/A**	**Current Issue**
Trojan.Portacopo:br	**N/A**	**Current Issue**
Trojan.Prova	N/A	CyberNotes-2002-10
Trojan.PSW.CrazyBilets	N/A	CyberNotes-2002-12
Trojan.PSW.M2	N/A	CyberNotes-2002-13
Trojan.Starfi	**N/A**	**Current Issue**
VBS.Gascript	N/A	CyberNotes-2002-04
VBS.Zevach	N/A	CyberNotes-2002-15
VBS_CHICK.B	N/A	CyberNotes-2002-07
VBS_THEGAME.A	N/A	CyberNotes-2002-03
W32.Alerta.Trojan	N/A	CyberNotes-2002-05
W32.Azak	**N/A**	**Current Issue**
W32.Cbomb	**N/A**	**Current Issue**
W32.Click	N/A	CyberNotes-2002-15
W32.Delalot.B.Trojan	N/A	CyberNotes-2002-06
W32.DSS.Trojan	N/A	CyberNotes-2002-09
W32.Estrella	N/A	CyberNotes-2002-13
W32.Evala.Worm	N/A	CyberNotes-2002-14
W32.IRCBot	N/A	CyberNotes-2002-14
W32.Kamil	**N/A**	**Current Issue**
W32.Kotef	**N/A**	**Current Issue**
W32.Libi	N/A	CyberNotes-2002-10
W32.Maldal.J	N/A	CyberNotes-2002-07
W32.Nuker.Winskill	N/A	CyberNotes-2002-15
W32.Tendoolf	N/A	CyberNotes-2002-09
W32.Wabbin	N/A	CyberNotes-2002-15
WbeCheck	N/A	CyberNotes-2002-09
Winshell	N/A	CyberNotes-2002-15

AIM-Flood: This is a Trojan programmed to steal password information for AOL Instant Chat clients. This Trojan requires VB40032.DLL in order to perform its malicious actions. In testing, this Trojan modified the WIN.INI file to run the file:

- C:\windows\system\system.exe

This file was not created and does not exist by default.

Backdoor.Delf: This is a Backdoor Trojan that allows unauthorized access to the infected computer. It will also stop the process of some antivirus and firewall software. Backdoor.Delf works only on Windows NT, 2000, and XP systems. It allows a malicious user to access the compromised system without authorization. It attempts to steal the infected computers Windows and Dial-up passwords. The Trojan copies itself as %windir%\System32\Scanvegw.exe. So that it runs when you start Windows, it adds the value, “Windows Service,” to one or more of these registry keys:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServicesOnce
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce

Backdoor.Delf.B (Alias: Backdoor.Delf.bv): This is a Backdoor Trojan that allows unauthorized access to the infected computer. It will also stop the process of some antivirus and firewall software. It works on Windows NT, 000, and XP systems Backdoor.Delf.B allows a malicious user to access the compromised system without authorization. The Trojan copies itself as %windir%\System\Kernel32.exe. So that it runs when Windows is started, it adds the value "LoadWindowsFile" to these registry keys:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

and references the dropped file.

Backdoor.Easyserv (Alias: Backdoor.Easyserv.): This is a backdoor Trojan that gives a malicious user limited access to a compromised computer. When it is activated, Backdoor.Easyserv does the following: It listens on port 5558 for a connection. Once connected, the malicious user can direct Backdoor.Easyserv to activate an HTTP server that will show the directory structure of any local hard disk. The HTTP server will allow the malicious user to connect to the host machine using an Internet browser. Through the browser, the malicious user can browse the host computer and download files from it. Backdoor.Easyserv creates the string value "easyServ   <path to server.exe>\Server.exe" under the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Backdoor.Easyserv does not display any indication that it is running.

Backdoor.Fearic (Alias: Backdoor.Fear.15): This is a backdoor Trojan horse that allows a malicious user to use America Online Instant Messenger (AIM) or to open TCP/UDP ports to gain control of a computer. It is written in the Microsoft Visual Basic (VB) programming language. It will listen on ports 8811, 3456, and 2000.

Backdoor.Kavar: This is a backdoor Trojan that also has the capability to download other Trojans or variants of this Trojan from the malicious user's ftp site. When it is executed, it copies itself as %windir%\Kv3000v.exe and runs as a service. It then adds a value "Kervarsystem %windir%\kv3000v.exe" in the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

This Trojan also creates the file %windir%\Kervar3232.ini.

Backdoor.MLink: This Trojan horse allows unauthorized access to the infected computer. It is the server portion of a backdoor Trojan. The client access is configurable, and no static ports are used. When running, the Trojan copies itself as %windir%\System\Magiclink.exe. It also creates the file %windir%\System\Systemdllxpc.vxd, which is only an information file. So that it runs when you start Windows, the Trojan creates the value "Magic Link Server %windir%\system\Magiclink.exe" in the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

Backdoor.WinShell: This is a server program that allows unauthorized access to the infected computer. It creates a server for backdoor access using Telnet. The ports are configurable. This Trojan allows Windows Shell access by Command.com, Cmd.exe, and other shell programs, which obtain full access to files and programs. When the program is installed, it creates the value "WinShell   <Original location and file name of the Trojan>" in the following registry keys:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

The Trojan does not drop or rename files.

FakeGina.Trojan: This is a Password Stealer Trojan. It steals the infected systems user name, domain, and passwords. This Trojan is a .dll file. For the Trojan to work, it must be manually copied to the System32 folder or to any folder that is in the Windows path. In addition, the value "GinaDLL fakegina.dll" must be added to the registry key:

- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

Following this, when the computer is restarted, the Trojan will capture all your successful logins (domains, user names and passwords) and write them to the file Passlist.txt.

IRC.kierz (Alias: Trojan.IRC.KarmaHotel.b): This is a Trojan that spreads using mIRC. It spreads across mIRC channels. It creates these files, which are deleted after the script runs:

- C:\Rol.vbs
- C:\Mirc.dat
- C:\Winamod.ini

The script searches all folders for Mirc.ini and overwrites that file to configure remote=on.

PWS-Ritter: This is a password stealing Trojan designed to capture the login password of NetWare 3.11 users. The file name "LOGIN.EXE" is used by the Trojan, as a replacement for the standard LOGIN binary when connecting to a Novell NetWare server. The date and time stamp of this Trojan is October 19, 1994 9:27 PM, but this can be easily altered.

StartPage-B (Aliases: BackDoor.Pyand, Trojan.Win32.StartPage.b): This Trojan is compressed with the UPX packer. When run, it will modify the Internet Explorer start page setting. This is accomplished by changing a setting in the registry. The start page is set to a Russian web page, http://yandex.8n.com. This website will redirect to www.porta.ru/index.html.

Troj/Tobizan-A: This is a backdoor Trojan that creates a copy of itself named kernel32.exe in the Windows system folder and adds the following registry entries to ensure that this file is run each time Windows is started:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run\kernel32
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\kernel32

The Trojan allows a remote malicious user to communicate with and control the compromised computer using IRC.

Troj/Unreal-A: This Trojan has been reported in the wild. It is an executable that displays the brief message "Installing Unreal Tournament 2003 15daycrack" and extracts a number of files to a subfolder named system under the standard Windows System folder. The Trojan then reboots the computer without warning. Among the extracted files are svchost.exe, explorer.exe, iw.dll, several INI (mIRC script) files and a registry file named svchost.reg. The dropper imports svchost.reg that adds the following entries to the registry:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall\mIRC DisplayName = "mIRC"
- HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall\mIRC UninstallString = "SVCHOST.EXE -uninstall"

To launch itself at Windows Startup, the Trojan adds the registry entry:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run svchost =

Explorer.exe is passed svchost.exe on the command line to launch that executable. Explorer.exe is not viral; its function is to launch an application and immediately hide the main window. If svchost.exe is executed from the command line or from the Windows shell, it appears to be a mIRC-like chat program. When launched using the dropped explorer.exe, it runs invisibly. In both cases, the Trojan listens on port 59 and the identd port for TCP connections. The process is visible and can be killed using the Task Manager under all versions of Windows.

Trojan.Junnan: This is a Trojan horse that causes a picture and sound to appear at regular intervals on an infected computer. There is no destructive payload, but the program configures itself to run when Windows is started, without the consent or knowledge of the user. It is a nuisance program that, at regular intervals, displays a picture accompanied by a triumphant yell. It originated in Asia. The Trojan adds the value. “junnan <file name of the originally executed Trojan>” to the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Current Version\Run

so that it runs each time that you start Windows. There are no other modifications to system files, and the Trojan does not drop or copy files to a set location. There is no destructive payload, other than the interruption caused by the pop-up window.

Trojan.Portacopo:br: This is a Trojan horse that destroys files on an infected system. It only affects systems that use localized Portuguese (Brazilian) settings. When it is run, it copies itself as C:\%Windir%\Wsys.exe. The Trojan creates the value “Boot Verify C:\%windir%\Wsys.exe /plus” in the registry key:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

So that it runs when Windows is started. The Trojan displays messages that contain Portuguese text. When the bottom in the message boxes is clicked, the Trojan will open or close the CD-ROM drive.
The Trojan's payload is to overwrite all unopened files under all folders and subfolders in the local hard drives and network drives. The overwritten files are all 1 byte in length.

Trojan.Starfi: This is a Trojan horse that is written in Visual Basic. The Trojan is designed to steal passwords from MSN Messenger users. Once the Trojan is running on the system, a malicious user can send commands to infected computers and obtain their MSN Messenger login name and password. Trojan.Starfi attempts to disguise itself as a picture. When it is executed, it displays the following fake error message:

- Internal Error. Picture could not be shown #0003421.

If the file is executed on a computer that does not have MSN Messenger installed, a Windows error message will appear. In this case, the Trojan will not do anything on the system. Due to bugs in the Trojan, MSN Messenger may not work properly after infection. In most cases, removing the Trojan will fix the problem.

W32.Azak: This is a Trojan Horse that copies itself to all local drives as three files whose file names begin with "KaZaa." This Trojan has no payload.

W32.Cbomb: This is a Trojan horse and worm that moves all files from the \Windows\System folder to the Windows desktop, and moves the desktop files to the C:\Cbomb folder. W32.Cbomb is written in Visual Basic. When it is first executed, it displays a dialog box prompting you to enter a number. Next a message box is displayed. Finally, if the number that you entered in the first dialog box was "4,” it displays a message indicating that the bomb timer has been successfully completed. The Trojan also attempts to use Microsoft Outlook to send itself to all addresses in the Microsoft Outlook Address book. The e-mail has the following characteristics:

- Subject: Dear My Friend <intended recipient's user name>
- Message: I have send you an attachment that I made with Macromedia Flash 6.0. It's about Brittany Spear <offensive word removed> with Me.
- Attachment: <variable filename with an .exe extension>

However, the e-mail routine does not work successfully.

W32.Kamil: This is a Trojan horse that attempts to download a variant of W32.BleBla worm from the Internet. It also moves all files from the Windows and Desktop folders to the C:\Nur_Mohd_Kamil folder, which is created by W32.Kamil and is very similar to W32.Cbomb.

W32.Kotef: This is a Trojan that attempts to copy itself as these files:

- C:\Korea.exe
- C:\Windows\Korea.exe
- C:\Japan.exe
- C:\Winnt\Korea.exe
- C:\Windows\Startm~1\Programs\Startup\Ktf.exe

When W32.Kotef runs, it does the following:

- It displays a dialog box that has two buttons.
- If you click one of the buttons, the Trojan displays a picture file.
- If you click the other button, the Trojan copies the binary code starting at offset 32768 of the Trojan file to the end of the Trojan file, and copies this into a file that has the same name as the original file, but with the .vir extension. For example, if the original file name is Korea.exe, with a file size of 122,880 bytes, the Trojan creates the file Korea.vir that contains the binary data from offset 32768 to 122880 from the file Korea.exe.

It also attempts to modify the Autoexec.bat file to copy the file A:\Secret.exe to C:\Korea.exe. The Trojan also attempts to add the value “KTF_Love_Imel” with a value data of either “C:\Windows\Korea.exe” or “C\Winnt\Korea.exe” to the registry key:

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

It also attempts to create the file C:\Run32.vbs, which adds two URL link files to the Windows desktop. The first of these URL files contains a link to the virus author's Web site, and the second contains a link to send mail to the virus author. The Trojan also attempts to create the file C:\RunVbs.bat, which executes C:\Run32.vbs.